Rekall Release notes

DFRWS 2017 Release - Codenamed Hurricane Ridge

Last week at DFRWS 2017, we were proud to launch Rekall 1.7.0RC1 with the first alpha release of the Rekall Agent. The Rekall Agent is a distributed end point monitoring solution based on the Google Cloud Platform. The launch also includes a white paper and a demo site hosted at https://dfrws2017-rekall.appspot.com.

Apart from its scalability, enterprise grade access control and auditing, the Rekall Agent brings the capabilities of both Rekall's EFilter query language as well as OSQuery's capabilities into a complete distributed endpoint monitoring solution. The overall solution makes it possible to launch a flexible query on many endpoint systems at the same time, and collect their responses quickly and efficiently.

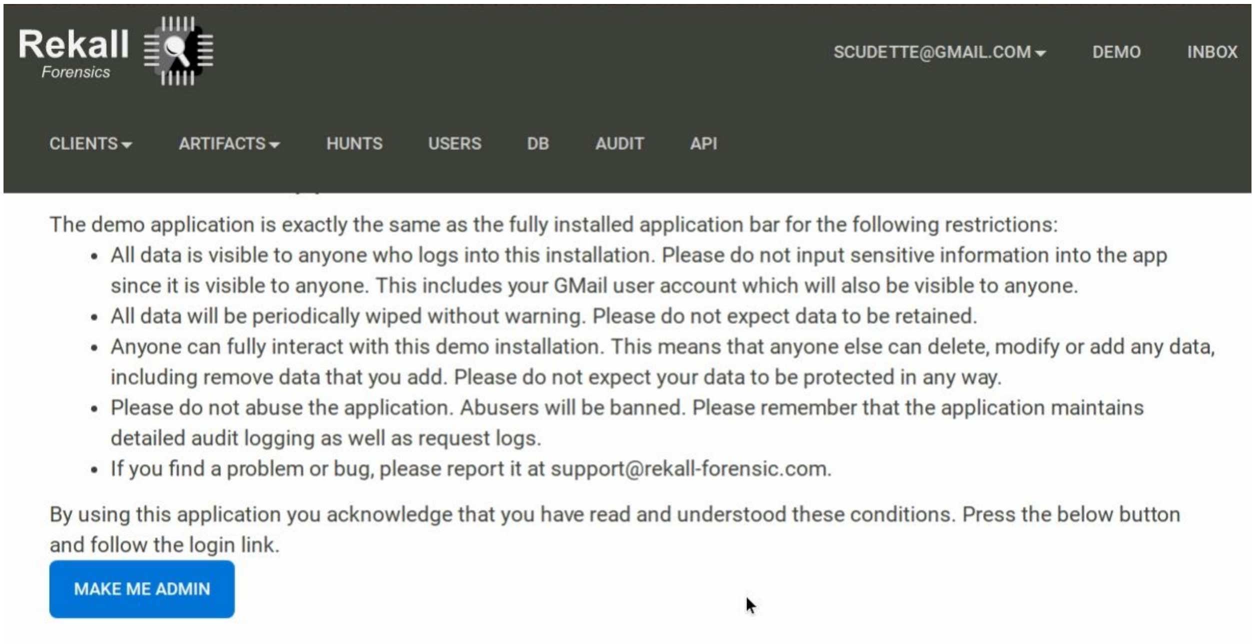
At DFRWS we worked through a hands on workshop where participants installed the Rekall Agent server on their own Google Cloud project, or alternatively we used a shared project for collaborative remote forensic investigations. We then ran through a number of common forensic and incident response scenarios.

The workshop had been so successful that people have requested the project to remain up after the workshop, so they could continue playing with the release.

Rekall Agent demo site

We have decided therefore to leave the site up as a demo site. This means anyone from the internet can request administrator rights for the application and quickly see how it works.

Simply navigate to https://dfrws2017-rekall.appspot.com/ and you should see the agreement page. Please note that since this is a shared system (in which anyone is an admin level user), all data can be viewed by anyone else.



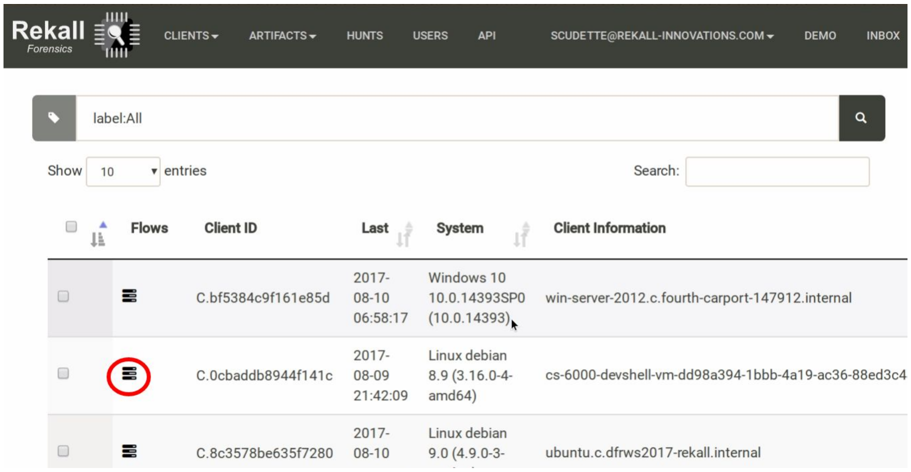
The demo application is exactly the same as the fully installed application bar for the following restrictions:

- All data is visible to anyone who logs into this installation. Please do not input sensitive information into the app since it is visible to anyone. This includes your GMail user account which will also be visible to anyone.
- All data will be periodically wiped without warning. Please do not expect data to be retained.
- Anyone can fully interact with this demo installation. This means that anyone else can delete, modify or add any data, including remove data that you add. Please do not expect your data to be protected in any way.
- Please do not abuse the application. Abusers will be banned. Please remember that the application maintains detailed audit logging as well as request logs.
- If you find a problem or bug, please report it at support@rekall-forensic.com.

By using this application you acknowledge that you have read and understood these conditions. Press the below button and follow the login link.

By clicking the **Make Me Admin** button, the application will assign the **Administrator** and **Viewer** roles to your username. The Viewer role is needed so you can login and search for clients. The Administrator role allows you to assign any other roles to your username as needed.

Let's start off by searching for clients (For a small installation such as this, simply search for label:All to list all the clients):



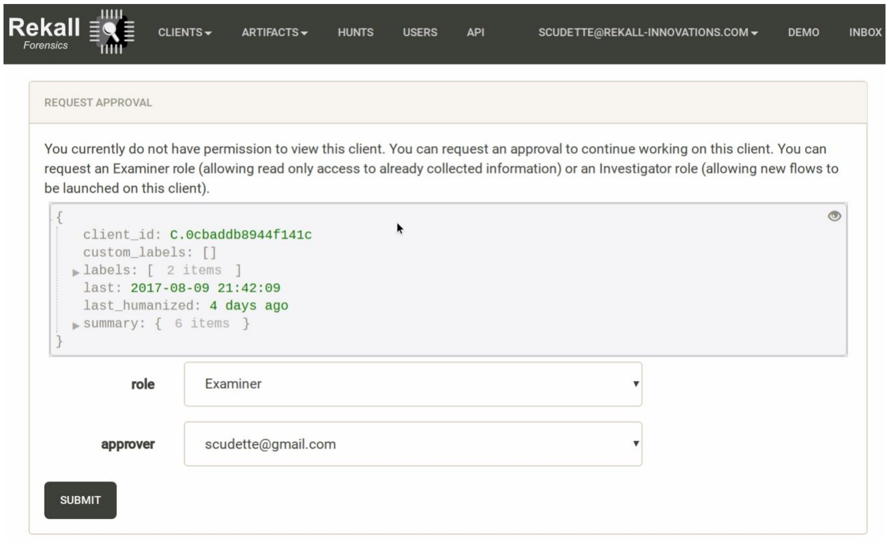
label:All

Show 10 entries

Search:

□	Flows	Client ID	Last	System	Client Information
□	☰	C.bf5384c9f161e85d	2017-08-10 06:58:17	Windows 10 10.0.14393SP0 (10.0.14393)	win-server-2012.c.fourth-carport-147912.internal
□	☰	C.0cbaddb8944f141c	2017-08-09 21:42:09	Linux debian 8.9 (3.16.0-4-amd64)	cs-6000-devshell-vm-dd98a394-1bbb-4a19-ac36-88ed3c4
□	☰	C.8c3578be635f7280	2017-08-10	Linux debian 9.0 (4.9.0-3-	ubuntu.c.dfrws2017-rekall.internal

Now to view the flows in each client, simply click on the flows column.



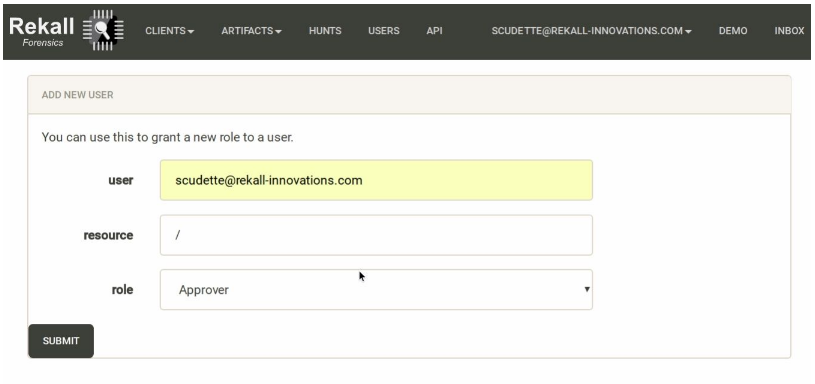
REQUEST APPROVAL

You currently do not have permission to view this client. You can request an approval to continue working on this client. You can request an Examiner role (allowing read only access to already collected information) or an Investigator role (allowing new flows to be launched on this client).

```
{
   client_id: C.0cbaddb8944f141c
   custom_labels: []
 ▸ labels: [ 2 items ]
   last: 2017-08-09 21:42:09
   last_humanized: 4 days ago
 ▸ summary: { 6 items }
}
```

role	Examiner
approver	scudette@gmail.com

Since you do not currently have approval to access this client, the UI will start the approval request workflow. You can request an Examiner (read only) or Investigator (can launch flows) roles on this client. The approver list shows all users with approver rights. If you do not appear in this list you will need to grant yourself the approver role by clicking the **USERS** menu then **Add**:

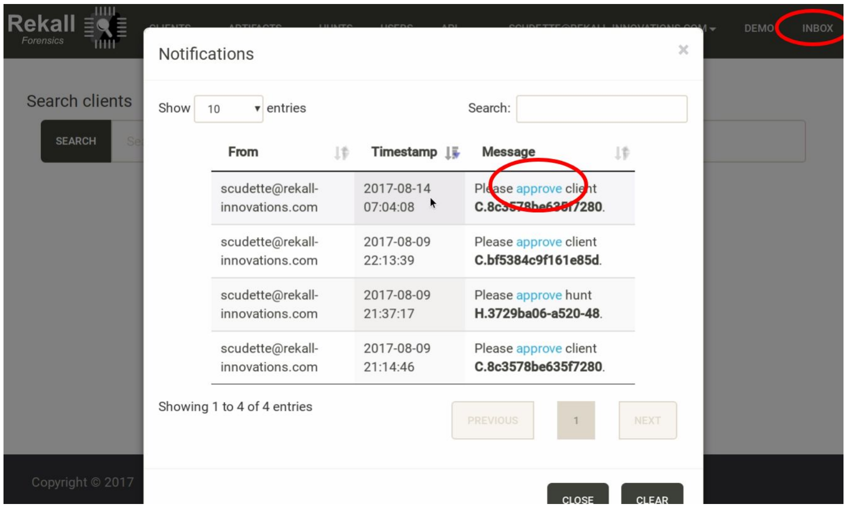


ADD NEW USER

You can use this to grant a new role to a user.

user	scudette@rekall-innovations.com
resource	/
role	Approver

Once the approval request is sent, you can see it in your inbox at the top right of the screen.



Notifications

Show 10 entries Search:

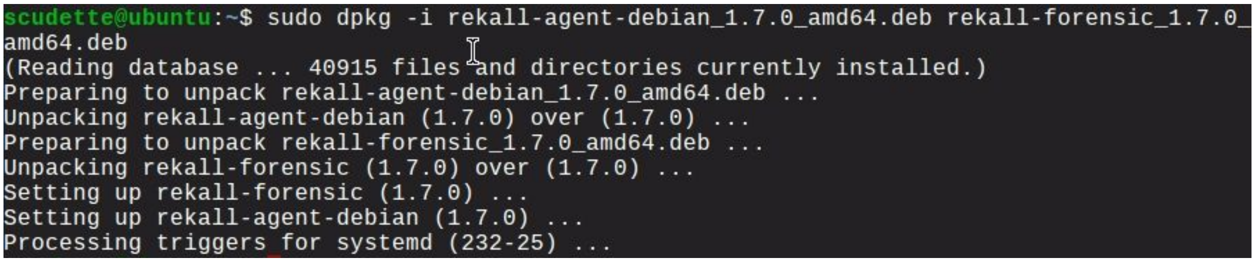
From	Timestamp	Message
scudette@rekall-innovations.com	2017-08-14 07:04:08	Please approve client **C.8c3578be635f7280**.
scudette@rekall-innovations.com	2017-08-09 22:13:39	Please approve client **C.bf5384c9f161e85d**.
scudette@rekall-innovations.com	2017-08-09 21:37:17	Please approve hunt **H.3729ba06-a520-48**.
scudette@rekall-innovations.com	2017-08-09 21:14:46	Please approve client **C.8c3578be635f7280**.

Showing 1 to 4 of 4 entries

Adding new machines to the demo site

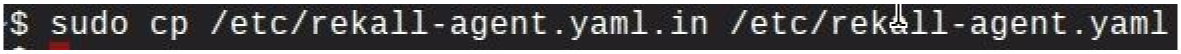
You are welcome to add new agent machines to the Rekall demo site, and use the demo site to run Rekall plugins on them. Note that since this is a shared site and you are effectively granting it root access you should only use disposable machines (e.g. VMs). In fact you should probably run the agent as a non-root user.

First install both the Rekall Agent and Rekall Forensic packages as distributed above



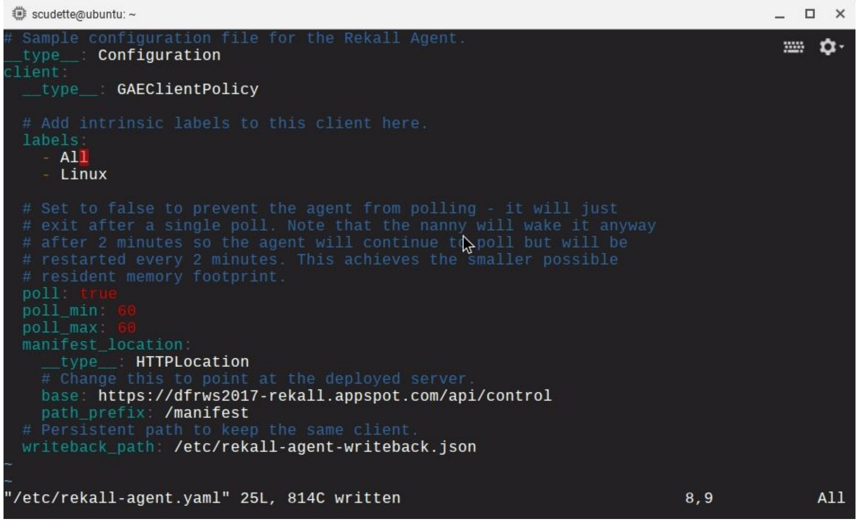
```
scudette@ubuntu:~$ sudo dpkg -i rekall-agent-debian_1.7.0_amd64.deb rekall-forensic_1.7.0_
amd64.deb
(Reading database ... 40915 files and directories currently installed.)
Preparing to unpack rekall-agent-debian_1.7.0_amd64.deb ...
Unpacking rekall-agent-debian (1.7.0) over (1.7.0) ...
Preparing to unpack rekall-forensic_1.7.0_amd64.deb ...
Unpacking rekall-forensic (1.7.0) over (1.7.0) ...
Setting up rekall-forensic (1.7.0) ...
Setting up rekall-agent-debian (1.7.0) ...
Processing triggers for systemd (232-25) ...
```

Then copy the sample configuration file:



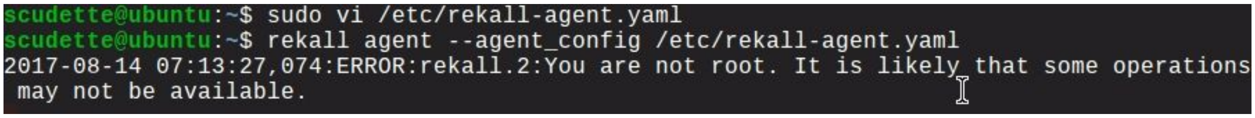
```
$ sudo cp /etc/rekall-agent.yaml.in /etc/rekall-agent.yaml
```

And replace the location with the demo site:



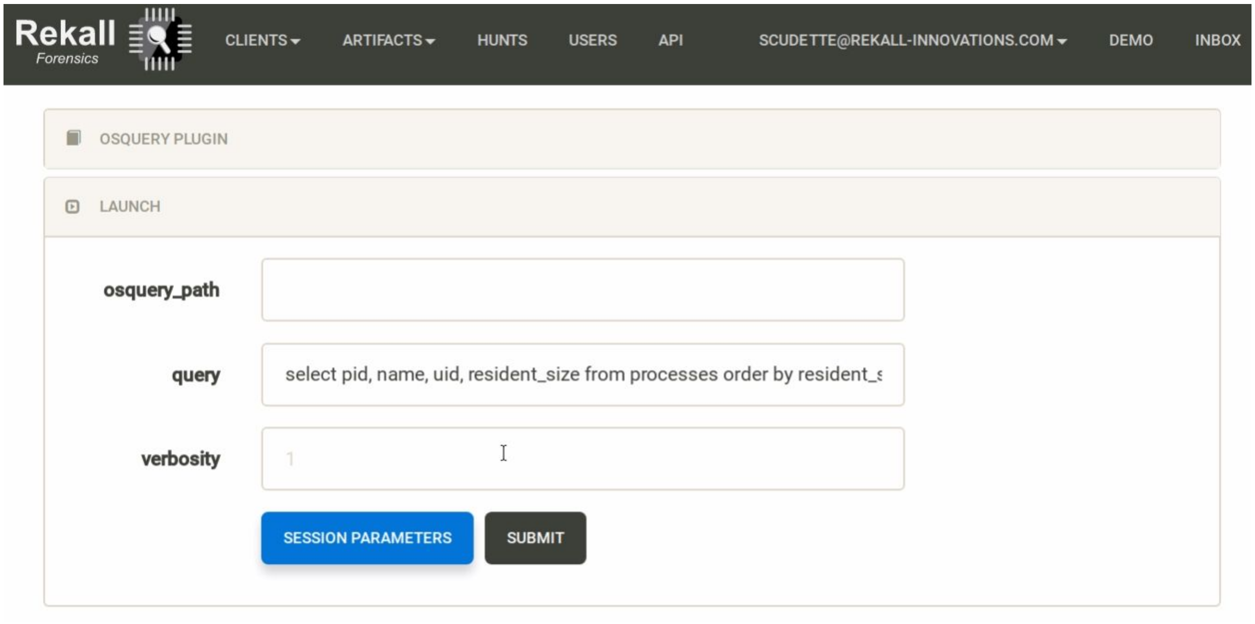
```
# Sample configuration file for the Rekall Agent.
__type__: Configuration
client:
  __type__: GAEClientPolicy

  # Add intrinsic labels to this client here.
  labels:
    - All
    - Linux

  # Set to false to prevent the agent from polling - it will just
  # exit after a single poll. Note that the nanny will wake it anyway
  # after 2 minutes so the agent will continue to poll but will be
  # restarted every 2 minutes. This achieves the smaller possible
  # resident memory footprint.
  poll: true
  poll_min: 60
  poll_max: 60
  manifest_location:
    __type__: HTTPLocation
    # Change this to point at the deployed server.
    base: https://dfrws2017-rekall.appspot.com/api/control
    path_prefix: /manifest
  # Persistent path to keep the same client.
  writeback_path: /etc/rekall-agent-writeback.json
~
~
"/etc/rekall-agent.yaml" 25L, 814C written                    8,9           All
```

You should run the agent as non root by hand using the command line (you may need to change the writeback path to somewhere it can write to):



```
scudette@ubuntu:~$ sudo vi /etc/rekall-agent.yaml
scudette@ubuntu:~$ rekall agent --agent_config /etc/rekall-agent.yaml
2017-08-14 07:13:27,074:ERROR:rekall.2:You are not root. It is likely that some operations
 may not be available.
```

Now you can launch any plugin against your client. For example, to launch an OSQuery query simply select the "osquery plugin" then enter the query:

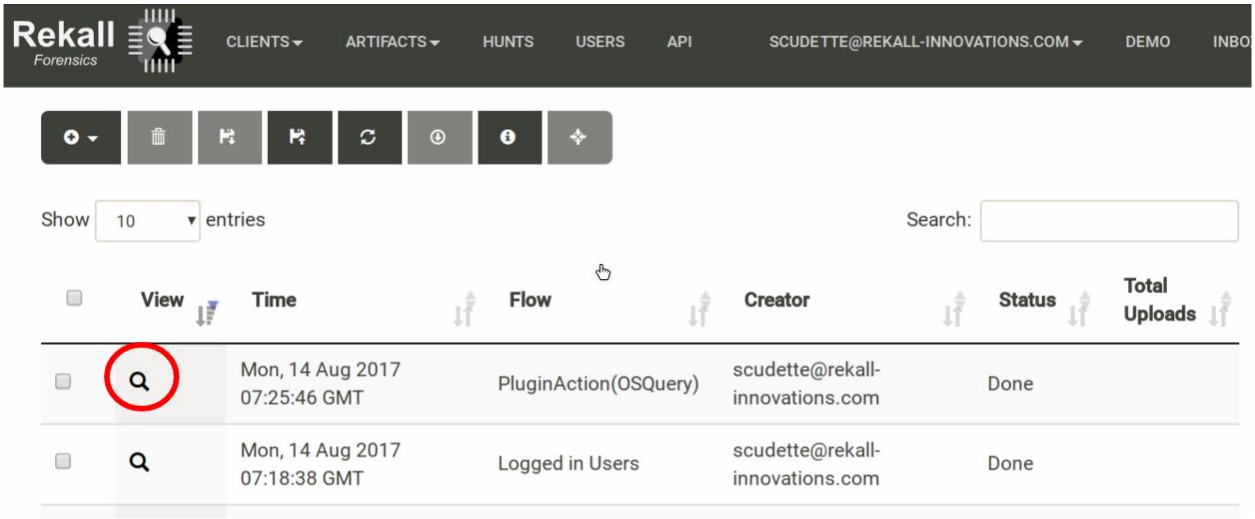


osquery_path:

query: select pid, name, uid, resident_size from processes order by resident_s

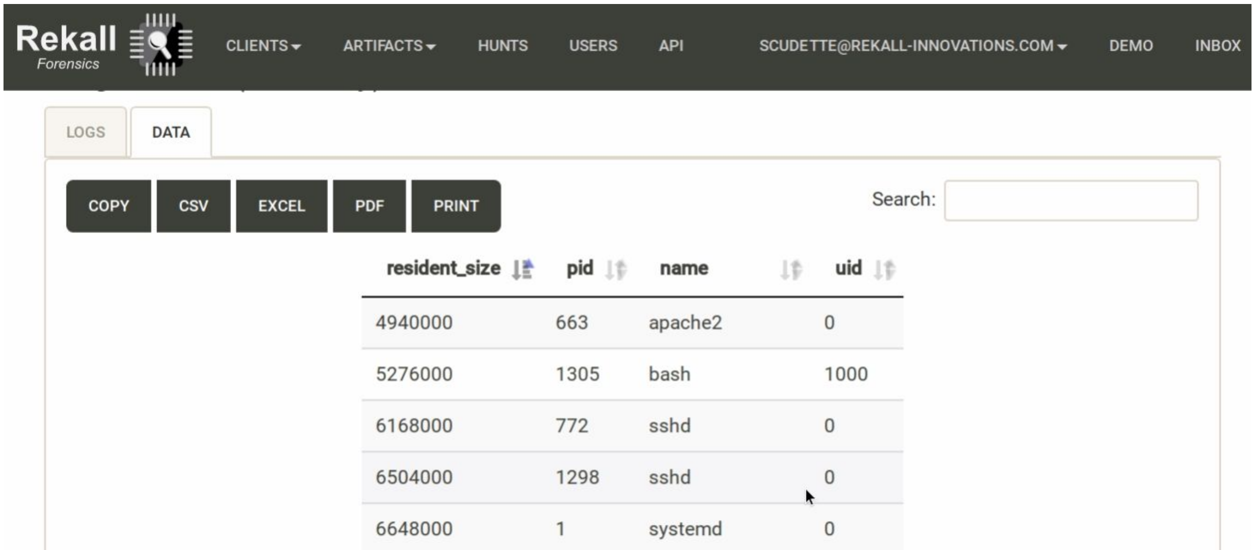
verbosity: 1

After waiting for the Agent to pick up the new query, the flow will be marked as **Done**:



□	View	Time	Flow	Creator	Status	Total Uploads
□	🔍	Mon, 14 Aug 2017 07:25:46 GMT	PluginAction(OSQuery)	scudette@rekall-innovations.com	Done	
□	🔍	Mon, 14 Aug 2017 07:18:38 GMT	Logged in Users	scudette@rekall-innovations.com	Done	

We can view the collection which is the result of the query



resident_size	pid	name	uid
4940000	663	apache2	0
5276000	1305	bash	1000
6168000	772	sshd	0
6504000	1298	sshd	0
6648000	1	systemd	0

Feedback

This is the first Alpha release of Rekall Agent - we put it out there to solicit comments, thoughts and discussions. Please mail us at rekall-discuss@googlegroups.com with any suggestions for further improvements.